

① 13

Original document

RADIO TAG SECURITY EXTENSION METHOD, ID MANAGEMENT COMPUTER SYSTEM, PROXY SERVER DEVICE, THEIR PROGRAMS, AND RECORDING MEDIUM OF PROGRAMS

Publication number: JP2004318645

Publication date: 2004-11-11

Inventor: KINOSHITA SHINGO; HOSHINO FUMISATO; KOMURO TOMOYUKI; FUJIMURA AKIKO

Applicant: NIPPON TELEGRAPH & TELEPHONE

Classification:

- international: **G06K17/00; H04L9/32; G06K17/00; H04L9/32**; (IPC1-7): G06K17/00; H04L9/32

- European:

Application number: JP20030113798 20030418

Priority number(s): JP20030113798 20030418

[View INPADOC patent family](#)

[View list of citing documents](#)

[Report a data error here](#)

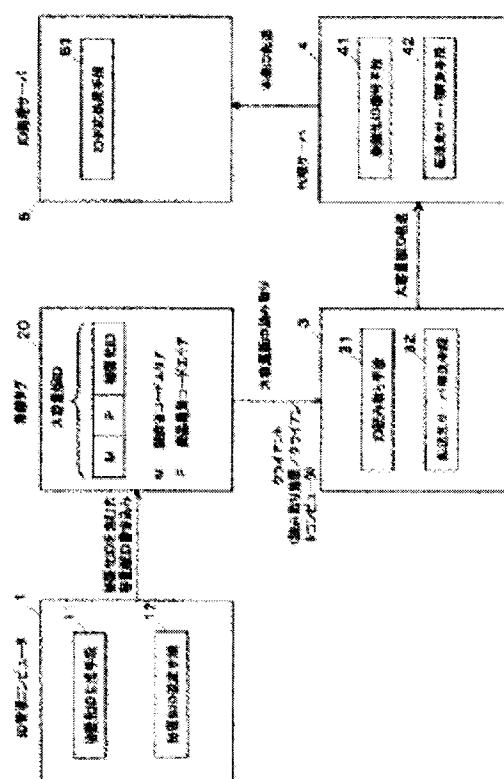
Abstract of JP2004318645

PROBLEM TO BE SOLVED: To protect privacy relating to the ID of a radio tag and to improve the security of the radio tag.

SOLUTION: An ID management computer 1 conceals a small capacity version ID indicating an original product identification electronic code (EPC), turns it to a secret ID, sets it in the individual number area of the large capacity version ID of the radio tag 20, and sets information whose transmission destination is a proxy server 4 in the area of a manufacturer code and a product kind code. A client 3 reads the large capacity version ID from the radio tag 20 and transfers the large capacity version ID to the proxy server 4. The proxy server 4 restores the original small capacity version ID by decoding the secret ID set to the received large capacity version ID and transfers the decoded original small capacity version ID to an ID processing server 5 which processes the ID from the

manufacturer code and the product kind code.

COPYRIGHT: (C)2005,JPO&NCIPI



Data supplied from the *esp@cenet* database - Worldwide

JP2004318645: No description available

Data supplied from the *esp@cenet* database - Worldwide

JP2004318645: No claims available

Data supplied from the *esp@cenet* database - Worldwide

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-318645

(P2004-318645A)

(43) 公開日 平成16年11月11日(2004. 11. 11)

(51) Int. Cl.⁷
G06K 17/00
H04L 9/32

F I

G06K 17/00 T
G06K 17/00 F
H04L 9/00 673C

テーマコード (参考)

5B058
5J104

審査請求 未請求 請求項の数 14 O L (全 17 頁)

(21) 出願番号 特願2003-113798 (P2003-113798)
(22) 出願日 平成15年4月18日 (2003. 4. 18)

(71) 出願人 000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号
(74) 代理人 100087848
弁理士 小笠原 吉義
(74) 代理人 100074848
弁理士 森田 寛
(74) 代理人 100095072
弁理士 岡田 光由
(72) 発明者 木下 真吾
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内
(72) 発明者 星野 文学
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

最終頁に続く

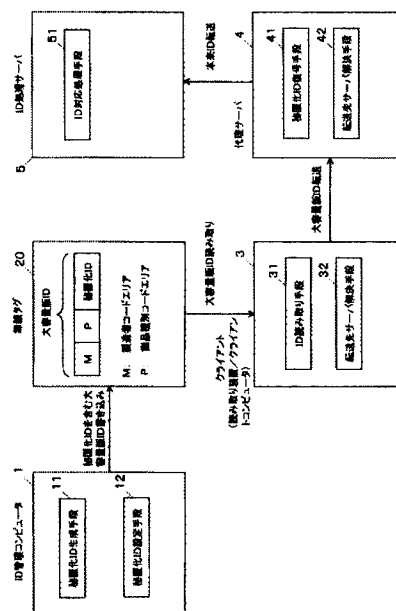
(54) 【発明の名称】 無線タグセキュリティ拡張方法、ID管理コンピュータ装置、代理サーバ装置、それらのプログラムおよびそれらのプログラムの記録媒体

(57) 【要約】

【課題】無線タグのIDに関するプライバシー保護を図り、無線タグのセキュリティを向上させる。

【解決手段】ID管理コンピュータ1は、本来の商品識別電子コード(EPC)を示す小容量版IDを秘匿化して秘匿化IDとし、無線タグ20の大容量版IDの個体番号エリアに設定し、製造者コード、商品種別コードのエリアに代理サーバ4を送信先とする情報を設定する。クライアント3は、無線タグ20から大容量版IDを読み取り、代理サーバ4に大容量版IDを転送する。代理サーバ4は、受信した大容量版IDに設定されている秘匿化IDを復号して本来の小容量版IDを復元し、その製造者コード、商品種別コードからIDを処理するID処理サーバ5へ復号した本来の小容量版IDを転送する。

【選択図】 図1



【特許請求の範囲】**【請求項1】**

無線タグから読み取った識別コードを、その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおける無線タグセキュリティ拡張方法であって、

所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第1の識別コードを秘匿化したコードと、所定の代理サーバ装置を送信先として特定するための送信先特定情報とを含む第2の識別コードを生成し、無線タグに設定する過程と、

前記無線タグから第2の識別コードを読み取り、前記送信先特定情報を用いて前記代理サーバ装置へ第2の識別コードを送信する過程と、

前記代理サーバ装置において第2の識別コードから秘匿化された第1の識別コードを復号する過程と、

復号した第1の識別コードに含まれる送信先特定情報に基づいて特定のサーバ装置へ第1の識別コードを送信する過程とを有することを特徴とする無線タグセキュリティ拡張方法。

【請求項2】

無線タグから読み取った識別コードを、その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおける無線タグセキュリティ拡張方法であって、

所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第1の識別コードに、正当性認証用の認証子を付与したコードと、所定の代理サーバ装置を送信先として特定するための送信先特定情報とを含む第2の識別コードを生成し、無線タグに設定する過程と、

前記無線タグから第2の識別コードを読み取り、前記送信先特定情報を用いて前記代理サーバ装置へ第2の識別コードを送信する過程と、

前記代理サーバ装置において第2の識別コードに含まれる認証子から該識別コードの正当性を検証する過程と、

検証した結果、正当であると判定された場合に、前記第1の識別コードに含まれる送信先特定情報に基づいて特定のサーバ装置へ第1の識別コードを送信する過程とを有することを特徴とする無線タグセキュリティ拡張方法。

【請求項3】

無線タグから読み取った識別コードを、その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおける無線タグセキュリティ拡張方法であって、

所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第1の識別コードを秘匿化したコードと、正当性認証用の認証子と、所定の代理サーバ装置を送信先として特定するための送信先特定情報とを含む第2の識別コードを生成し、無線タグに設定する過程と、

前記無線タグから第2の識別コードを読み取り、前記送信先特定情報を用いて前記代理サーバ装置へ第2の識別コードを送信する過程と、

前記代理サーバ装置において第2の識別コードに含まれる認証子から該識別コードの正当性を検証する過程と、

検証した結果、正当であると判定された場合に、第2の識別コードから秘匿化された第1の識別コードを復号する過程と、

復号した第1の識別コードに含まれる送信先特定情報に基づいて特定のサーバ装置へ第1の識別コードを送信する過程とを有することを特徴とする無線タグセキュリティ拡張方法。

【請求項4】

請求項1、請求項2または請求項3記載の無線タグセキュリティ拡張方法において、

前記第1の識別コードは、商品識別電子コードであり、
前記送信先を特定するための送信先特定情報は、商品識別電子コードにおける製造者コードエリアまたはその製造者コードエリアと商品種別コードエリアとに設定される情報であることを特徴とする無線タグセキュリティ拡張方法。

【請求項5】

無線タグから読み取った識別コードを、その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおいて無線タグに識別コードを設定するID管理コンピュータ装置であって、
所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第1の識別コードを秘匿化したコードと、所定の代理サーバ装置であって前記秘匿化したコードを復号する代理サーバ装置を送信先として特定するための送信先特定情報とを含む第2の識別コードを生成する秘匿化識別コード生成手段と、
生成した第2の識別コードを、前記第1の識別コードによる識別対象となる個体に添付する無線タグに設定する秘匿化識別コード設定手段とを備えることを特徴とするID管理コンピュータ装置。

【請求項6】

無線タグから読み取った識別コードを、その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおいて無線タグに識別コードを設定するID管理コンピュータ装置であって、
所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第1の識別コードに、正当性認証用の認証子を付与したコードと、所定の代理サーバ装置であって前記認証子を用いて該識別コードの正当性を検証する代理サーバ装置を送信先として特定するための送信先特定情報とを含む第2の識別コードを生成する認証子付き識別コード生成手段と、
生成した第2の識別コードを、前記第1の識別コードによる識別対象となる個体に添付する無線タグに設定する認証子付き識別コード設定手段とを備えることを特徴とするID管理コンピュータ装置。

【請求項7】

無線タグから読み取った識別コードを、その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおいて無線タグに識別コードを設定するID管理コンピュータ装置であって、
所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第1の識別コードを秘匿化したコードと、正当性認証用の認証子と、所定の代理サーバ装置であって前記認証子を用いて該識別コードの正当性を検証するとともに前記秘匿化したコードを復号する代理サーバ装置を送信先として特定するための送信先特定情報とを含む第2の識別コードを生成する識別コード生成手段と、
生成した第2の識別コードを、前記第1の識別コードによる識別対象となる個体に添付する無線タグに設定する識別コード設定手段とを備えることを特徴とするID管理コンピュータ装置。

【請求項8】

無線タグから読み取った識別コードを、その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおける代理サーバ装置であって、
無線タグから識別コードを読み取った装置から、所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第1の識別コードを秘匿化したコードを含む第2の識別コードを受信する秘匿化識別コード受信手段と、
受信した第2の識別コードから秘匿化された第1の識別コードを復号する秘匿化識別コード復号手段と、
復号した第1の識別コードに含まれる送信先特定情報に基づいて特定のサーバ装置へ第1の識別コードを送信する識別コード転送手段とを備えることを特徴とする代理サーバ装置

。

【請求項9】

無線タグから読み取った識別コードを、その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおける代理サーバ装置であって、

無線タグから識別コードを読み取った装置から、所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第1の識別コードに、正当性認証用の認証子を付与したコードを含む第2の識別コードを受信する認証付き識別コード受信手段と、

受信した第2の識別コードに含まれる認証子から該識別コードの正当性を検証する識別コード検証手段と、

検証した結果、正当であると判定した場合に、前記第1の識別コードに含まれる送信先特定情報に基づいて特定のサーバ装置へ第1の識別コードを送信する識別コード転送手段とを備えることを特徴とする代理サーバ装置。

【請求項10】

無線タグから読み取った識別コードを、その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおける代理サーバ装置であって、

無線タグから識別コードを読み取った装置から、所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第1の識別コードを秘匿化したコードと、正当性認証用の認証子とを含む第2の識別コードを受信する識別コード受信手段と、受信した第2の識別コードに含まれる認証子から該識別コードの正当性を検証する識別コード検証手段と、

検証した結果、正当であると判定した場合に、前記第2の識別コードから秘匿化された第1の識別コードを復号する秘匿化識別コード復号手段と、

復号した第1の識別コードに含まれる送信先特定情報に基づいて特定のサーバ装置へ第1の識別コードを送信する識別コード転送手段とを備えることを特徴とする代理サーバ装置。

。

【請求項11】

請求項5、請求項6または請求項7記載のID管理コンピュータ装置が備える前記各手段をコンピュータによって実現するための、コンピュータに実行させるID管理コンピュータ装置用プログラム。

【請求項12】

請求項8、請求項9または請求項10記載の代理サーバ装置が備える前記各手段をコンピュータによって実現するための、コンピュータに実行させる代理サーバ装置用プログラム。

。

【請求項13】

請求項5、請求項6または請求項7記載のID管理コンピュータ装置が備える前記各手段をコンピュータによって実現するための、コンピュータに実行させるプログラムを記録した

ことを特徴とするID管理コンピュータ装置用プログラムの記録媒体。

【請求項14】

請求項8、請求項9または請求項10記載の代理サーバ装置が備える前記各手段をコンピュータによって実現するための、コンピュータに実行させるプログラムを記録したことを特徴とする代理サーバ装置用プログラムの記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、無線タグセキュリティ技術に関し、特に、無線タグを利用した自動認識システムにおいて、無線タグに関するプライバシー保護、無線タグの偽造／なりすまし防止を実現

する方法に関するものである。

【0002】

【従来の技術】

商品などの自動認識システムを低コストで実現するために、無線タグに固有のID（識別コード）のみを格納し、それを商品に貼り付け、読み取り装置でIDを読み取り、商品関連情報は、ネットワーク側で管理するというアプローチが取られている。

【0003】

例えば、米国のマサチューセッツ工科大学（MIT）によるAutoIDセンター（<http://www.autoidcenter.org>）では、商品のコード体系として、製造者コードと、商品の種別を示す商品種別コードと、商品個体の番号を示す個体番号とからなるIDを用い、そのIDだけを無線タグに格納し、商品関連情報を無線タグに格納したIDに関連付けてネットワーク上のコンピュータで管理することが考えられている。このシステムでは、商品関連情報に関するセキュリティは、ネットワーク側のセキュリティ技術を適用することにより確保されているが、無線タグのID読み取り制限などのセキュリティについては対処されていない（例えば、非特許文献1参照）。

【0004】

【非特許文献1】

MIT AUTO-ID CENTER, "TECHNOLOGY GUIDE",
[online], [平成15年3月18日検索], インターネット<URL: http://www.autoidcenter.org/new_media/brochures/Technology_Guide.pdf>

【0005】

【発明が解決しようとする課題】

上記従来技術の方法では、無線タグからのID読み取り制限がなされておらず、読み取り装置を保有する者であれば誰でもIDを読み取ることができるため、消費者などの所有品情報が漏洩してしまうという問題がある。さらに、製造者コードや商品種別コードを入手できた場合、適当な商品個体コードを推測し無線タグに書き込むことによって、無線タグの偽造／なりすましにより容易に商品の偽造などが可能になってしまうといった問題もある。

【0006】

本発明は、上記問題を解決するものであり、無線タグのID自体を秘匿化することにより、所有者のプライバシーを保護する手段、および無線タグのIDに認証子を付加することにより、IDの偽造／なりすましを防止する手段を低コストで提供することを目的とする。

【0007】

【課題を解決するための手段】

本発明は、上記課題を解決するため、例えば以下の構成を採る。ここでは、無線タグに設定される識別コードとして商品識別電子コード（以下、EPCともいう）の例を用いて説明する。商品識別電子コードには、データ長が異なる小容量版ID（例：96ビット）と大容量版ID（例：256ビット）の少なくとも2種類以上があり、それぞれ無線タグを添付する商品の製造者コードと、商品の種別を示す商品種別コードと、商品個体のシリアル番号を示す個体番号のエリアを有するものとする。

【0008】

図1は、第1の本発明の構成の一例を示す図である。1はID管理コンピュータ、3は無線タグの読み取り装置または読み取り装置付きクライアントコンピュータ（以下、クライアントという）、4はクライアント3およびサーバ5の双方と通信可能なコンピュータを備える代理サーバ、5はIDに基づくデータの加工や保管などの処理を行うコンピュータを備えるID処理サーバである。また、20は商品に貼られる無線タグである。

【0009】

ID管理コンピュータ1内において、11は秘匿化ID生成手段、12は秘匿化ID設定手段である。クライアント3内において、31は無線タグ20のID読み取り手段、32

は転送先サーバ解決手段である。代理サーバ4内において、41は秘匿化ID復号手段、42は転送先サーバ解決手段である。ID処理サーバ5内において、51はID対応処理手段である。

【0010】

ID管理コンピュータ1は、秘匿化ID生成手段11を利用し、本来の商品識別電子コードを示す小容量版IDを秘匿化した秘匿化IDを生成する。秘匿化ID設定手段12は、生成した秘匿化IDを無線タグ20が有する大容量版IDの個体番号のエリアに書き込み、また、大容量版IDの製造者コードおよび商品種別コードのエリアに、代理サーバ4を送信先として特定することのできる商品情報とは無関係なコードを格納する。例えば製造者コードには、代理サーバ4を運営する第三者機関の会社コードを、商品種別コードには、ID秘匿化サービスを示すコードを格納する。

【0011】

クライアント3は、ID読み取り手段31により、無線タグ20から秘匿化IDを含む大容量版IDを読み取り、IDの製造者コードあるいは商品種別コードに基づき、転送先サーバ解決手段32によって、アドレス解決サーバなどを別途利用するなどして、転送先サーバを決定する。もし、無線タグ20から読み取ったIDが、秘匿化前の小容量版IDであった場合には、ID処理サーバ5が転送先サーバとなるが、秘匿化IDを書き込んで生成された大容量版IDの場合には、製造者コード、商品種別コードから代理サーバ4が転送先サーバとして決定されることになる。なお、図1において図示省略したアドレス解決サーバは、あらかじめ定められた製造者コード、商品種別コードと、転送先サーバのアドレス(IPアドレス等)とを対応付ける手段を持っており、製造者コード、商品種別コードによるアドレス解決要求に対して、製造者コード、商品種別コードから転送先サーバのアドレスを決定し、アドレス解決の要求元へ回答する。

【0012】

クライアント3は、転送先サーバである代理サーバ4へ、秘匿化IDを含む大容量版IDを転送する。代理サーバ4は、受信した大容量版IDの秘匿化IDを、秘匿化ID復号手段41により復号し、本来の小容量版IDを生成し、転送先サーバ解決手段42を用いて、小容量版IDから解決される本来の転送先であるID処理サーバ5を決定し、小容量版IDをID処理サーバ5へ転送する。ID処理サーバ5は、ID対応処理手段51を用いて、IDの保管や加工などの処理を行う。なお、クライアント3、代理サーバ4間の通信は認証、アクセス制御、暗号化など、何らかのセキュアな通信手段が提供されていることを前提としている。

【0013】

ID管理コンピュータ1の秘匿化ID生成手段11が、小容量版IDの秘匿化を実現する方法としては、共通鍵暗号方式や公開鍵暗号方式を用いて暗号化する方法を用いることができる。この場合、代理サーバ4の秘匿化ID復号手段41は、暗号化された小容量版IDを共通鍵または秘密鍵を用いて復号する。また、小容量版IDの秘匿化を実現する方法として、ID管理コンピュータ1と代理サーバ4との間で、任意に定めたユニークなコードと小容量版IDとの対応情報をテーブル化して管理し、これらの対応情報を共有することにより、ID管理コンピュータ1では、小容量版IDを任意のコードに置き換えることにより秘匿化し、代理サーバ4では、任意のコードから小容量版IDを復号する方法を用いることもできる。

【0014】

図2は、第2の本発明の構成の一例を示す図である。6はID管理コンピュータ、7はクライアント3およびID処理サーバ5の双方と通信可能なコンピュータを備える代理サーバ、21は無線タグである。クライアント3、ID処理サーバ5は第1の本発明と同様である。また、ID管理コンピュータ6内の61は認証子付きID生成手段、62は認証子付きID設定手段であり、代理サーバ7内の71は認証子付きID検証手段、72は転送先サーバ解決手段である。

【0015】

第2の本発明においては、ID管理コンピュータ6内の認証子付きID生成手段61は、小容量版IDの認証子を生成して小容量版IDに付加し、認証付きIDとする。認証子付きID設定手段62は、無線タグ21が有する大容量版IDの個体番号に認証子付きIDを書き込み、また、大容量版IDの製造者コードおよび商品種別コードのエリアに、代理サーバ7を送信先として特定することのできる商品情報とは無関係なコードを格納する。例えば製造者コードには、代理サーバ7を運営する第三者機関の会社コードを、商品種別コードには、ID認証サービスを示すコードを格納する。

【0016】

クライアント3は、ID読み取り手段31により、無線タグ21から認証子付きIDを含む大容量版IDを読み取り、IDの製造者コードあるいは商品種別コードに基づき、転送先サーバ解決手段32によって、アドレス解決サーバなどを別途利用するなどして、転送先サーバを決定する。ここで、無線タグ21から読み取ったIDが、認証子付きIDを含む大容量版IDの場合には、製造者コード、商品種別コードから代理サーバ7が転送先サーバとして選択されることになる。クライアント3は、認証子付きIDを含む大容量版IDを代理サーバ7へ転送する。

【0017】

代理サーバ7内の認証子付きID検証手段71は、受信した認証子付きIDを検証し、正規IDと判定した場合に、大容量版IDから本来の小容量版IDを抽出し、第1の本発明と同様に転送先サーバ解決手段72によって転送先サーバのアドレス解決を行い、ID処理サーバ5へ本来の小容量版IDを転送する。ID処理サーバ5の動作は、第1の本発明と同様である。

【0018】

認証子付きID生成手段61による小容量版IDの認証子生成は、小容量版IDの暗号処理（例えば、MAC（Message Authentication Cord）生成、デジタル署名など）により実現することができる。この認証子は、小容量版IDをもとにMACやデジタル署名によって生成されたメッセージダイジェストであり、署名データになる。代理サーバ7は、元の小容量版IDと認証子とを入力として、元の小容量版IDが改竄されていないかどうかを確認することができる。その認証に必要となる情報に、鍵を利用するアルゴリズムなどが必要であるが、これらの情報については、ID管理コンピュータ6と代理サーバ7との間で何らかの手段で共有しておく。共有方法は、安全に共有できる方法であればどのような方法でもよい。

【0019】

また、小容量版IDの認証子として、任意の認証子データを用意し、代理サーバ7において、本来の小容量IDとその認証子データとの対応情報を管理し、クライアント3からの要求に応じて対応関係を検証する方法を用いることもできる。

【0020】

第3の本発明は、上記第1の本発明と第2の本発明とを組み合わせた手段を持つ発明である。ID管理コンピュータでは、本来の商品コードを示す小容量版IDを秘匿化すると同時に、秘匿化した小容量版IDの認証子を生成して、秘匿化した小容量版IDに付加し、無線タグが有する大容量版IDの個体番号のエリアに書き込み、また、大容量版IDの製造者コードおよび商品種別コードのエリアに商品情報と無関係な送信先特定情報を格納する。この場合の送信先特定情報として、IDの認証と秘匿化IDの復号とを行う代理サーバが転送先サーバとして決定されるような情報を設定する。

【0021】

以上のように、本発明によれば、本来のIDが秘匿化されて格納されているため、第三者により不正に読み取りされた場合でも、第三者は本来のIDを認識することができず、所有品情報などの漏洩を防ぐことが可能となる。また、本来のIDが認証子付きで格納されているため、代理サーバ7にて本来のIDの認証が可能となり、IDの偽造やなりすましを防ぐことが可能となる。

【0022】

【発明の実施の形態】

本発明をMITのオート(Auto)IDシステムに適用した例に従って、本発明の実施の形態を説明する。図3は、本発明の第1の実施の形態におけるシステムの全体構成の一例を示したものである。図3に示すシステムにおいて、1は小容量版IDを秘匿化し、無線タグ20の大容量版ID内に書き込むID管理コンピュータである。また、無線タグ20は、商品2に貼られており、無線タグの読み取り装置33を備えたクライアントコンピュータ30と、ID(EPC)データを格納するPML(Physical Markup Language)サーバ8と、IDから、そのIDデータを格納するPMLサーバ8のアドレスを解決するONS(Object Naming Service)サーバ9と、秘匿化IDの復号処理などを行う代理サーバ4とが、インターネット10により接続されている。

【0023】

説明を簡単にするために、ここでは、秘匿化IDの生成と秘匿化IDを無線タグ20に書き込む処理とを、1台のコンピュータによるID管理コンピュータ1で行う例を示しているが、秘匿化IDを生成する処理とそれを無線タグ20に書き込む処理とを分け、複数台のコンピュータによってID管理コンピュータ1を実現してもよい。

【0024】

はじめに、本発明の第1の実施の形態に関するEPC(Electronic Product Code)の格納方法を図4を用いて説明する。EPCは、AutoIDで用いるIDの名前である。EPCのコード体系として、種々のデータ長のものが規定されているが、本実施の形態では、96ビット版EPCを本来のID、256版EPCを秘匿化IDを含む大容量版IDとして用いることにする。

【0025】

図4(A)に示す96ビット版EPCは、バージョン番号8ビット、製造者コード28ビット、商品種別コード24ビット、個体番号36ビットからなる。図4では、例として、“ABC製薬”会社の製造者コード「0x1234567」，“薬XX”の商品種別コード「0xABCDEF」，個体番号「0x123456789」が格納されている様子を示している。

【0026】

この状態のままでは、消費者が薬をカバンに入れ持ち歩いているとき、第三者が読み取り装置33さえ持っていれば、EPCコードを読み取ることができ、その製造者コードと商品種別コードから、“ABC製薬”の“薬XX”を所有しているということが第三者にわかってしまう。

【0027】

本実施の形態では、図4(B)に示すように、ID管理コンピュータ1が、96ビットの本来のEPCを秘匿化し、図4(C)に示す256ビット版EPCの個体番号として格納する。秘匿化の例として、図4では、128ビット共通鍵暗号を利用している。このとき、256ビット版EPCの製造者コードおよび商品種別コードには、本来の商品のコードではなく、代理サーバ4をEPCの送信先として特定することができるコードを設定する。図4(C)の例では、製造者コードとして代理サーバ4を運営する“プライバシー保護社”のコード「0xABCDEF0123456789」が格納され、また、商品種別コードとして、無線タグの“ID秘匿化サービス”のコード「0x1234567890ABCD」が格納されている。

【0028】

なお、秘匿化の方法として、公開鍵暗号を利用することも可能である。また、任意のコードを埋め込み、それと本来の96ビット版EPCとの対応関係を代理サーバ4などに保有させておき、代理サーバ4にてID変換を行うという方法もある。すなわち、ID管理コンピュータ1と代理サーバ4との間で、任意のコードと96ビット版EPCとの変換テーブルを何らの方法で共有し、その変換テーブルを用いてID変換を行う方法を用いてもよい。

【0029】

さらに、図示していないが、秘匿化EPCの格納先として、個体番号領域だけでなく、商品種別コードの領域も合わせて利用することにより、より大きな秘匿化EPCデータをサポートすることもできる。また、商品種別コードに利用する秘匿化方法（暗号アルゴリズムや鍵IDなど）を含めることにより、複数の暗号方法や鍵を扱えるようにすることも可能である。

【0030】

次に、本発明の第1の実施の形態における本来の96ビット版EPCのシステム全体の処理シーケンスについて、図5に従って説明する。図3のシステムにおいて、無線タグ20内にID管理コンピュータ1が生成した256ビット版EPCではなく、図4(A)に示す本来の96ビット版EPCが格納されていた場合の処理シーケンスは、図5の(a1)～(a4)のようになる。この96ビット版EPCの処理シーケンスでは、代理サーバ4が関与することがなく、シーケンスは従来技術とまったく同様である。

【0031】

(a1) 読み取り装置33を内蔵した、クライアントコンピュータ30が、無線タグ20から本来の96ビット版EPCを読み取る。

【0032】

(a2) クライアントコンピュータ30は、ONSサーバ9に対して、EPCを送信し、それを送信すべき転送先サーバのアドレスの解決要求を行う。

【0033】

(a3) ONSサーバ9は、送信されてきたEPCに基づき、PMLサーバ8のアドレスを回答する。このとき、製造者コードあるいは商品種別コードなどをアドレス解決に用いる。アドレス解決の結果、本来のEPCの格納先であるPMLサーバ8（製造メーカ管理など）のアドレスが返される。

【0034】

(a4) クライアントコンピュータ30は、取得したアドレスに対して、EPCを送信する。PMLサーバ8は、受信したEPCを内部データ（XML形式など）として保管する。

【0035】

次に、本発明の第1の実施の形態におけるEPCを秘匿化した場合（秘匿化EPCを256ビット版EPCの個体番号に格納）の処理シーケンスを、図6に示す(b1)～(b9)に従って説明する。

【0036】

(b1) 読み取り装置33を内蔵したクライアントコンピュータ30が、秘匿化したEPCを格納した256ビット版EPC（図4(C)）を、無線タグ20から読み取る。

【0037】

(b2) クライアントコンピュータ30は、ONSサーバ9に対して、256ビット版EPCを送信し、それを送信すべき転送先サーバのアドレスの解決要求を行う。

【0038】

(b3) ONSサーバ9は、送信されてきたEPCの製造者コードあるいは商品種別コードに基づき、転送先サーバのアドレス（ここでは代理サーバ4のアドレス）を、要求元のクライアントコンピュータ30に回答する。

【0039】

(b4) クライアントコンピュータ30は、取得したアドレスに対して、秘匿化EPCを含む256ビット版EPCを送信する。

【0040】

(b5) 代理サーバ4は、受信した256ビット版EPCから、秘匿化された96ビット版EPCを取り出す。

【0041】

(b6) 代理サーバ4は、秘匿化EPCを復号することにより、本来の96ビット版EPCを得る。

【0042】

(b7) 次に、代理サーバ4は、本来のEPCをONSサーバ9へ送信し、対応する転送先サーバのアドレス解決要求を行う。

【0043】

(b8) ONSサーバ9は、受け取ったEPCの製造者コードあるいは商品種別コードに基づき、本来のEPCを処理するPMLサーバ8のアドレスを得て、そのPMLサーバ8のアドレスを代理サーバ4に回答する。

【0044】

(b9) 代理サーバ4は、そのPMLサーバ8に対して本来のEPCを送信し、PMLサーバ8は受信したEPCを内部データ(XML形式など)として保管する。

【0045】

ここで、クライアントコンピュータ30と代理サーバ4間は、クライアント認証付きのSSL(Secure Socket Layer)など、アクセス制御や通信路の暗号化、改竄検出などセキュアな通信路が別手段として提供されているものとする。

【0046】

次に、本発明をMITのオート(Auto)IDシステムに適用した第2の実施の形態を説明する。第2の実施の形態のシステム構成を、図7に示す。第2の実施の形態においても、基本的な構成は第1の実施の形態と同様である。第1の実施の形態との違いは、ID管理コンピュータ6が96ビット版EPCに認証子を付けることにより256ビット版EPCを生成し、無線タグ21に設定すること、代理サーバ7が、256ビット版EPCの認証子付きIDを検証することにより、無線タグ21から読み取ったEPCが正規IDであることを検証することである。

【0047】

本発明の第2の実施の形態に関するEPCの格納方法を、図8を用いて説明する。図8(A)に示す96ビット版EPCは、MITのオート(Auto)IDシステムで規定された本来の小容量版EPCであり、バージョン番号8ビット、製造者コード28ビット、商品種別コード24ビット、個体番号36ビットからなる。図8では、例として、“ABCバッグ”会社の製造者コード「0x2345678」、 “バッグXX”の商品種別コード「0xBCDEFG」、個体番号「0x234567891」が格納されている様子を示している。

【0048】

本実施の形態では、図8(B)に示すように、ID管理コンピュータ6が、本来の96ビット版EPCの認証子を生成する。この例では、認証子の生成に、ハッシュ関数の一つであるsha1(Secure Hash Algorithm 1)を用い、sha1の出力160ビットから64ビット分を切り出して、64ビットの認証子を生成している。ID管理コンピュータ6は、本来の96ビット版EPCに、生成した64ビットの認証子を付加し、図8(C)に示す256ビット版EPCの個体番号として格納する。

【0049】

このとき、256ビット版EPCの製造者コードおよび商品種別コードには、本来の商品のコードではなく、代理サーバ7をEPCの送信先として特定することができるコードを設定する。図4(C)の例では、製造者コードとして代理サーバ7を運営する“真贋判定社”のコード「0xBCDEFG01」が格納され、また、商品種別コードとして、“ID認証サービス”のコード「0x2345678910BCDE」が格納されている。

【0050】

なお、本システムにおいては、上記認証子の生成を暗号処理(例えば、MAC(Message Authentication Cord)生成、デジタル署名)により実現することも可能であり、また、認証子として任意のコードを用意し、それと本来のEPCとの対応関係を代理サーバ7に保有させておき、代理サーバ7にて対応関係を検証するという方法を採用することも可能である。

【0051】

次に、本発明の第2の実施の形態におけるEPCに認証子を付加した場合（認証子付きEPCを256ビット版EPCの個体番号に格納）の処理シーケンスを、図9に示す（c1）～（c9）に従って説明する。

【0052】

（c1）読み取り装置33を内蔵したクライアントコンピュータ30が、認証子付きEPCを格納した256ビット版EPC（図8（C））を、無線タグ21から読み取る。

【0053】

（c2）クライアントコンピュータ30は、ONSサーバ9に対して、256ビット版EPCを送信し、それを送信すべき転送先サーバのアドレスの解決要求を行う。

【0054】

（c3）ONSサーバ9は、送信されてきたEPCの製造者コードあるいは商品種別コードに基づき、転送先サーバのアドレス（ここでは代理サーバ7のアドレス）を回答する。

【0055】

（c4）クライアントコンピュータ30は、取得したアドレスに対して、認証子付きEPCを含む256ビット版EPCを送信する。

【0056】

（c5）代理サーバ7は、受信した256ビット版EPCから、認証子付きEPCを取り出す。

【0057】

（c6）代理サーバ7は、認証子付きEPCを認識子に基づいて検証する。

【0058】

（c7）代理サーバ7は、上記検証の結果、正規IDと判断した場合に、ONSサーバ9に対して認証子付きEPCの中の本来の96ビット版EPCを送り、転送先サーバのアドレス解決要求を行う。

【0059】

（c8）ONSサーバ9は、受け取った96ビット版EPCにおける製造者コードあるいは商品種別コードから、本来のEPCを処理するPMLサーバ8のアドレスを回答する。

【0060】

（c9）代理サーバ7は、そのPMLサーバ8に対して本来のEPCを送信し、PMLサーバ8は受信したEPCを内部データ（XML形式など）として保管する。

【0061】

本発明の第3の実施の形態では、上記第1の実施の形態におけるEPCの秘匿化と、第2の実施の形態における認証子の付加とを同時に行う。システム構成については、図3および図7と同様である。第3の実施の形態におけるID管理コンピュータの処理フローチャートを、図10に示す。

【0062】

ステップS1では、ID管理コンピュータは、無線タグの添付対象となる商品を識別する本来の96ビット版EPCを入力する。次に、ステップS2では、入力した本来の96ビット版EPCを所定の共通鍵または公開鍵などを用いて暗号化し、秘匿化EPCを生成する。ステップS3では、秘匿化EPCについてMAC生成やデジタル署名などの暗号処理により、認証子を生成する。

【0063】

ステップS4では、ステップS2、S3で生成した秘匿化EPCと認証子とを、256ビット版EPCの個体番号とする。ステップS5では、ID認証・秘匿化サービスに対してあらかじめ付与した固有の番号を、256ビット版EPCにおける商品種別コードとする。ステップS6では、代理サーバの運営会社に対してあらかじめ付与した固有の番号を、256ビット版EPCにおける製造者コードとする。なお、代理サーバの運営会社の番号およびID認証・秘匿化サービスの番号と、代理サーバのアドレス（IPアドレス）との対応情報は、あらかじめONSサーバに登録しているものとする。

【0064】

ステップS7では、EPCの世代またはデータ長などの種別を示すバージョン番号と、ステップS6で決定した製造者コードと、ステップS5で決定した商品種別コードと、ステップS4で決定した個体番号とを結合して、256ビット版EPCを生成する。ステップS8では、生成した256ビット版EPCを無線タグに書き込み、一つの無線タグへの書き込み処理を終了する。

【0065】

第3の実施の形態における代理サーバの処理フローチャートを、図11に示す。ステップS10では、クライアントコンピュータが無線タグから読み取った秘匿化EPCと認証子を含む256ビット版EPCを受信する。ステップS11では、受信した256ビット版EPCの個体番号から認証子を切り出し、正当なIDかどうかを検証する。ステップS12の判定により、検証した結果が正当でなければ、ステップS13へ進み、256ビット版EPCの送信元であるクライアントコンピュータへエラー通知を行い、処理を終了する。

【0066】

検証した結果、正当なIDであることがわかれば、ステップS14へ進み、256ビット版EPCの個体番号から秘匿化EPCを切り出して復号することにより、本来の96ビット版EPCを復元する。ステップS15では、96ビット版EPCをONSサーバへ送り、96ビット版EPCの製造者コード、商品種別コードによって定まるPMLサーバのアドレスを得る。ステップS16では、PMLサーバへ96ビット版EPCを送信し、処理を終了する。

【0067】

以上説明したID管理コンピュータおよび代理サーバの処理は、コンピュータとソフトウェアプログラムとによって実現することができ、そのプログラムをコンピュータ読み取り可能な記録媒体に記録して提供することも、ネットワークを通して提供することも可能である。

【0068】

【発明の効果】

以上説明したように、本発明によれば、無線タグには、添付対象を識別する本来のIDが秘匿化されて格納されており、その復号は、正規のコンピュータである代理サーバが自動的に呼び出されて行う仕組みを持つことにより、不正な第三者に対する無線タグのID情報漏洩を防止することができ、所有品情報などに関するプライバシーを保護することが可能となる。また、認証子付きのIDを格納することにより、IDが不正に生成され偽造商品などに貼り付けられている場合にも、ID偽造の検出が可能となり、偽造防止などが可能となる。

【図面の簡単な説明】

【図1】本発明の構成の一例を示す図である。

【図2】本発明の構成の一例を示す図である。

【図3】第1の実施の形態におけるシステムの全体構成の一例を示す図である。

【図4】秘匿化IDの格納方法を説明する図である。

【図5】本来の96ビット版EPCの処理シーケンスを示す図である。

【図6】秘匿化IDを含む256版EPCの処理シーケンスを示す図である。

【図7】第2の実施の形態におけるシステムの全体構成の一例を示す図である。

【図8】認証子付きIDの格納方法を説明する図である。

【図9】認証子付きIDの処理手順を説明するシーケンス図である。

【図10】第3の実施の形態におけるID管理コンピュータの処理フローチャートである。

【図11】第3の実施の形態における代理サーバの処理フローチャートである。

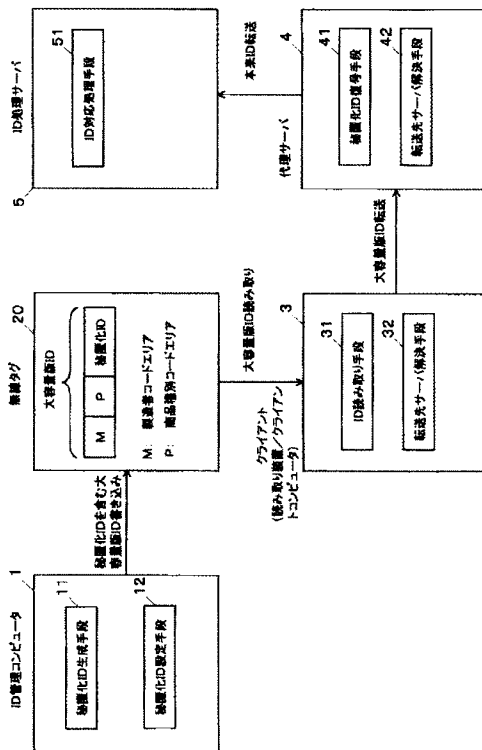
【符号の説明】

1, 6 ID管理コンピュータ

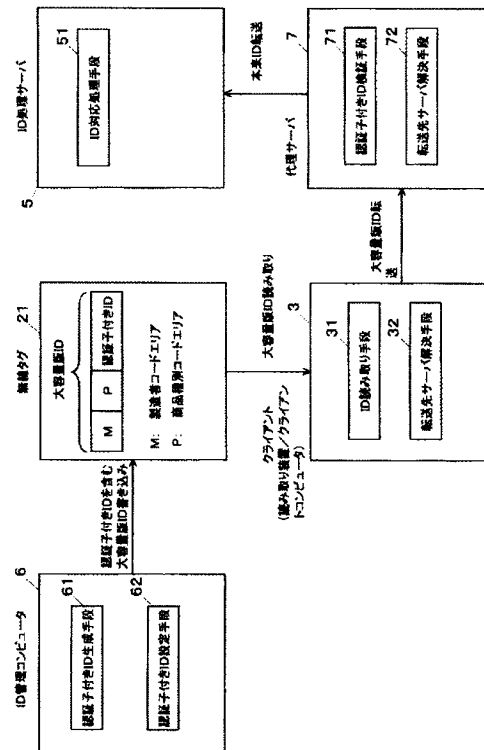
2 商品

- 3 クライアントコンピュータ
- 4, 7 代理サーバ
- 5 ID処理サーバ
- 8 PMLサーバ
- 9 ONSサーバ
- 10 インターネット
- 11 秘匿化ID生成手段
- 12 秘匿化ID設定手段
- 20, 21 無線タグ
- 30 クライアントコンピュータ
- 31 ID読み取り手段
- 32, 42, 72 転送先サーバ解決手段
- 33 読み取り装置
- 41 秘匿化ID復号手段
- 51 ID対応処理手段
- 61 認証付きID生成手段
- 62 認証付きID設定手段
- 71 認証付きID検証手段

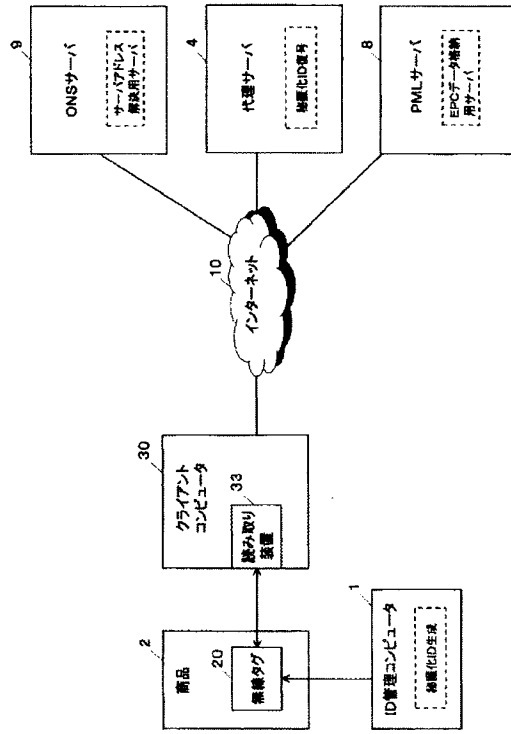
【図1】



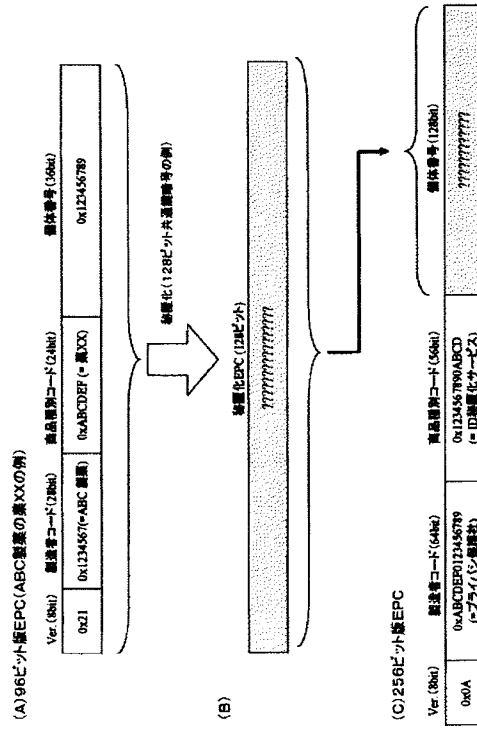
【図2】



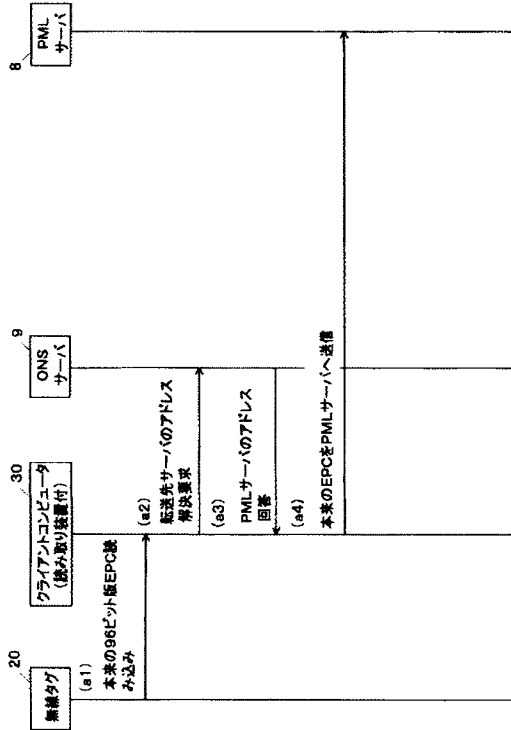
【図3】



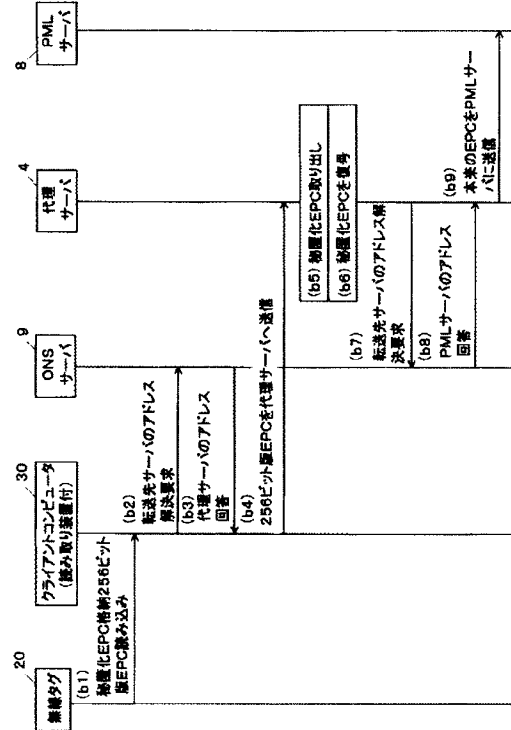
【図4】



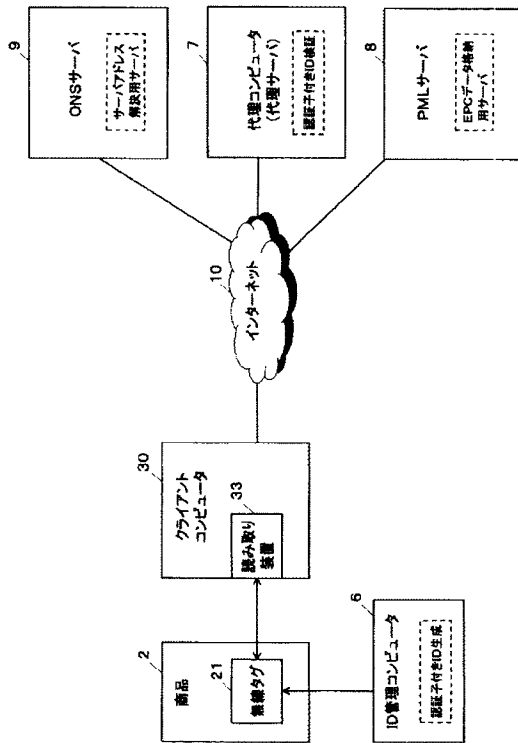
【図5】



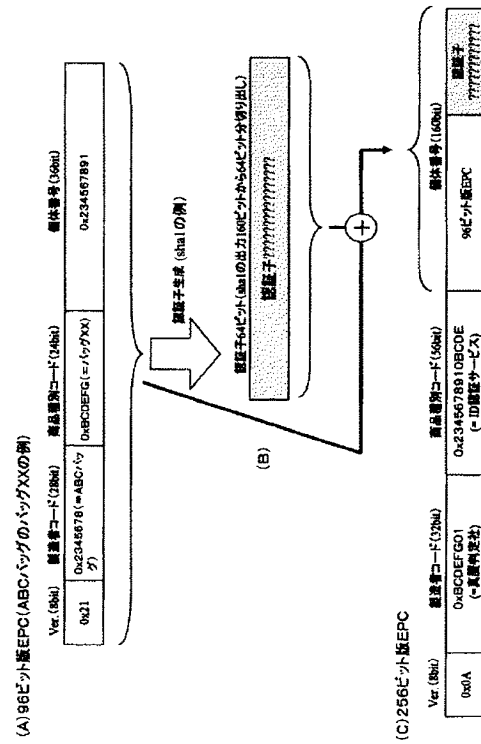
【図6】



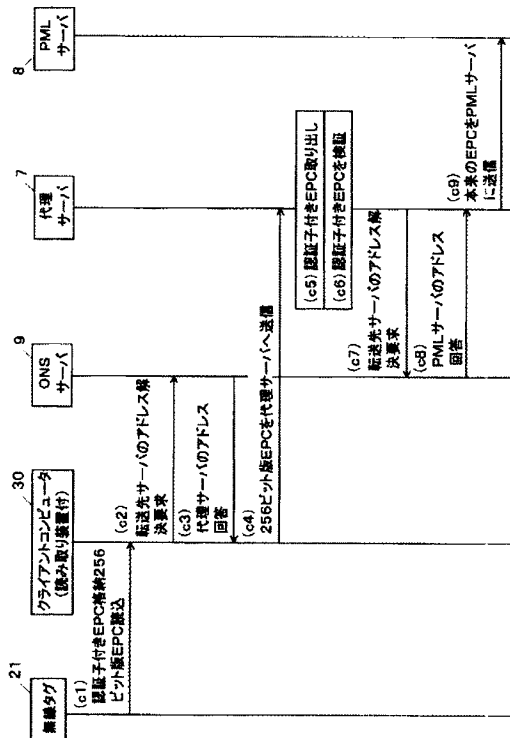
【図7】



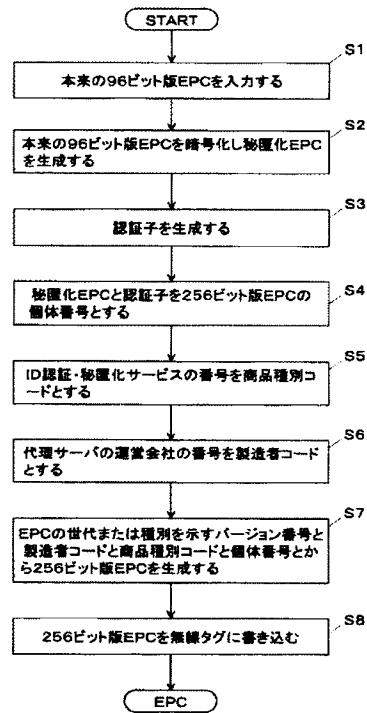
【図8】



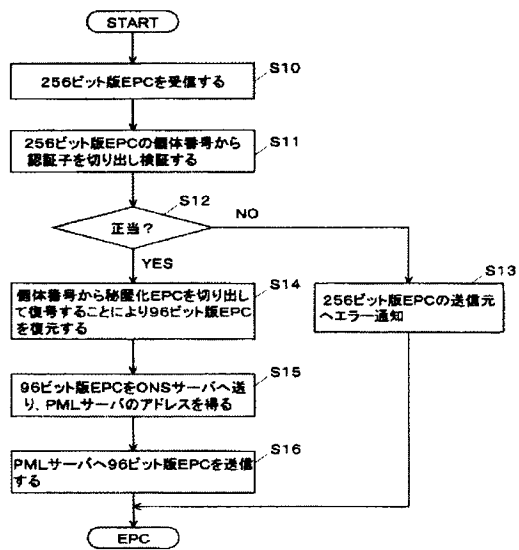
【図9】



【図10】



【図11】



(72)発明者 小室 智之

東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

(72)発明者 藤村 明子

東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

Fターム(参考) 5B058 CA01 CA15 KA32 KA33 YA20

5J104 AA07 KA02 KA04 KA15 NA02 NA05 NA27 NA38 PA07 PA10